

Appl. No. : 09/883,625
Filed : June 18, 2001

SUMMARY OF INTERVIEW

Exhibits and/or Demonstrations

None.

Identification of Claims Discussed

Claims 1, 4, 9, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23 were discussed during the interview.

Identification of Prior Art Discussed

U.S. Pat. No. 5,915,022 to Robinson was discussed during the interview.

Proposed Amendments

Applicant's representative submitted a proposed amendment in advance of the interview.

Principal Arguments and Other Matters

It was first noted that Claims 17-19 each include the feature of authentication by a third party, a feature not present in Robinson. The final Office Action did not accord these features patentable weight. Applicant's representative pointed out that in Applicant's response filed December 28, 2005, Applicant amended Claim 18 to provide a recitation of the third party in the body so that the Examiner would accord it patentable weight in its consideration. In addition, Applicant's representative pointed out that Claims 17 and 19 each include recitations of a third party outside the preamble of the claim. The Examiner agreed that the "third party" in each of these claims should be accorded patentable weight.

Differences between the remaining independent claims and Robinson was also discussed. In particular, it was pointed out that Robinson fails to show a system wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction as recited in Claim 20. Rather, the passages cited by the final Office Action differ from the language of the claims in that they show that a transaction certificate is decrypted by the first party to prove the transaction, not the second party as provided in Claim 20. For example, at column 6, lines 48-53, Robinson states:

Finally, in step 126, the customer preferably saves the confirmation page along with the encrypted transaction record appended thereto. As will be explained in further detail with respect to Figure 5, if the customer saves the confirmation page, he may later present it to the merchant in the event of a dispute over the transaction.

Appl. No. : 09/883,625
Filed : June 18, 2001

Thus, the customer in Robinson, e.g., the second party, saves the confirmation page along with the encrypted transaction. The second party does not decrypt the transaction certificate as recited in Claim 20.

It was further pointed out that the Office Action relies on Robinson's statement that a customer could hypothetically obtain the merchant's public key and could decrypt the transaction receipt to meet the feature of the second party using the decrypted proof elements to prove the transaction. See Robinson at column 5, lines 47-50. It was argued that Robinson does not go on to provide any description of how a customer, having obtained the merchant's public key and decrypted the transaction receipt to generate proof elements, could then use that those proof elements generated from the decrypted receipt to prove the transaction. Rather, any use of decrypted proof elements to prove the transaction in Robinson occurs only after the vendor decrypts the proof elements using its own private key. Applicant further noted that these arguments equally apply to the other independent claims.

During the interview the Examiner stated that although Robinson may not explicitly call out the second party using decrypted proof elements to prove the transaction, Robinson nevertheless anticipates the claims because the system described in Robinson could be used in the manner recited in the claims.

Results of Interview

Agreement was generally reached as to issues regarding according patentable weight to recitations of a third party not limited to the preamble (Claims 17-19). Agreement was not reached with respect to the remaining claims.

Appl. No. : 09/883,625
Filed : June 18, 2001

REMARKS

Applicant has reviewed the final Office Action mailed on March 14, 2006, and has considered the statements may by the Examiner during the telephonic interview on April 13, 2006, and these remarks are responsive thereto. Claims 1-23 remain pending in this application.

Discussion of Examiner Interview

Applicant's representative notes with appreciation the Examiner's willingness to conduct an interview to discuss the outstanding Office Action. Although agreement was not reached as to all issues, Applicant believes that the interview resulted in substantial progress in advancing the case.

Discussion of Cosmetic Amendments to Claims 16 and 17

Applicant has amended Claims 16 and 17 and notes that these amendments are for clarification purposes only and do not alter the scope of the claims. Applicant therefore respectfully requests that the Examiner enter these amendments prior to taking further action with respect to this case.

Discussion of Patentability of Claim Having a Third Party

Claims 17-19 each include the feature of "a third party, receiving an encrypted transaction certificate." As discussed during the interview, the final Office Action did not give patentable weight to the "third party" aspects of the claim. As was agreed during the telephonic interview, the "third party" features in these claims should be accorded patentable weight. Applicant submits that none of the cited references disclose a third party authenticating a transaction, and that Claims 17-19 are allowable for at least this reason.

Discussion of Claim Rejections under 35 U.S.C. § 102

Claims 4-5, 8, 15, 18, 20, and 22 stand rejected under 35 U.S.C. § 102(a), (e) as being anticipated by Robinson et al., U.S. Pat. No. 5,915,022 ("Robinson").

The Law of Anticipation

Appl. No. : 09/883,625
Filed : June 18, 2001

Anticipation under Section 102 can be found only if a reference shows exactly what is claimed. *Titanium Metals Corp. v. Banner*, 778 F.2d 775 (Fed. Cir. 1985). More particularly, a finding of anticipation requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention. *Electro Med. Sys. S.A. v. Cooper Life Sciences*, 34 F.3d 1048, 1052 (Fed. Cir. 1994). "To anticipate, every element and limitation of the claimed invention must be found in a single prior art reference, arranged as in the claim." *Brown v. 3M*, 265 F.3d 1349 (Fed. Cir. 2001). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970). Although the express, implicit, and inherent disclosures of a prior art reference may be relied upon in rejecting claims under section 102, the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. MPEP 2112; *In re Rijckaert*, 9 F.3d 1531, 1534 (Fed. Cir. 1993). Moreover, "the missing descriptive matter [must be] necessarily present in the thing described in the reference." *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999).

Applicant submits that each of claims 4-5, 8, 15, 18, 20, and 22 includes features related to a second party (e.g., a customer) decrypting proof elements and utilizing the decrypted proof elements to prove a transaction that are not disclosed, either explicitly or inherently, in Robinson.

Claim 20

Claim 20 stands rejected under Robinson. Claim 20 recites in part: "wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction." The Office Action states that Robinson shows instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate the decrypted selected elements, at column 5, lines 41-53. The Office Action further states that Robinson teaches that decrypted selected elements can be used by the second party to prove the transaction, at column 2, lines 31-43, at column 6, lines 23-67, and at column 7, lines 1-33.

Applicant submits that Robinson fails to show a system wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction as recited in Claim 20. Rather, the passages cited by the Office Action differ from the language of

Appl. No. : 09/883,625
Filed : June 18, 2001

the claims in that they show that a transaction certificate is decrypted by the first party to prove the transaction, not the second party as provided in Claim 20. For example, at column 6, lines 48-53, Robinson states:

Finally, in step 126, the customer preferably saves the confirmation page along with the encrypted transaction record appended thereto. As will be explained in further detail with respect to Figure 5, if the customer saves the confirmation page, he may later present it to the merchant in the event of a dispute over the transaction.

Thus, the customer in Robinson, e.g., the second party, saves the confirmation page along with the encrypted transaction. The second party does not decrypt the transaction certificate as recited in Claim 20.

Figure 1-2 in Robinson further confirms that it is the first party that decrypts the transaction certificate in order to prove the transaction rather than the second party as is recited in Claim 20. At blocks 124 and 126 in the figure, Robinson shows that a digital receipt page is received by the customer, e.g., the second party, and that the customer saves the digital receipt page. Nowhere in that figure does Robinson teach or suggest that the customer decrypts the encrypted transaction record and then uses that decrypted transaction record to prove the transaction. Further, at Figure 5, step 140, the customer presents the digital receipt page to the merchant, e.g., the first party. It is the merchant, e.g., the first party, who decrypts the transaction record at step 144 in Figure 5, not the customer.

As discussed above, a finding of anticipation requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention. The Examiner states in the final Office Action that “[i]f the prior art structure is capable of performing the intended use, then it meets the claim.” However, it is respectfully submitted that the Examiner fails to realize that the second party using the decrypted transaction record to prove the transaction is not intended use, but actual use. Claim 20 recites in relevant part “wherein the encrypted code attached to the transaction certificate is decrypted by the second party to prove the transaction.” Thus the use of the decrypted transaction certificate by the second party is not “intended use” as alleged by the Examiner, but rather is affirmatively carried out.

As discussed above, the fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish anticipation based on that reference. The characteristic must necessarily be present. The recited feature of “the encrypted code attached to

Appl. No. : 09/883,625
Filed : June 18, 2001

the transaction certificate is decrypted by the second party to prove the transaction" is not set forth in Robinson, nor does the Examiner point to why such a feature must be necessarily in the reference. Accordingly, the Examiner has not met his burden to establish that Robinson anticipates Claim 20, and therefore Claim 20 is allowable.

Claim 15

The Office Action also rejects Claim 15 as being anticipated by Robinson. Amended Claim 15 recites in part "decrypting by the second party the included encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action states that, at column 5, lines 47-50, Robinson teaches that a customer could obtain the merchant's public key and could be able to decrypt the transaction receipt. The Office Action further states that, at column 2, lines 31-43, column 6, lines 23-67, and column 7, lines 1-33, Robinson shows that decrypted proof elements are used to prove the transaction.

Applicant submits that Robinson fails to teach or otherwise disclose a system for decrypting "encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action relies on Robinson's statement that a customer could hypothetically obtain the merchant's public key and could decrypt the transaction receipt. However, Robinson does not go on to provide any description of how a customer, having obtained the merchant's public key and decrypted the transaction receipt to generate proof elements, could then use that those proof elements generated from the decrypted receipt to prove the transaction. Rather, any use of decrypted proof elements to prove the transaction in Robinson occurs only after the vendor decrypts the proof elements using its own private key. Thus, Robinson fails to teach at least these features, and Claim 15 is therefore allowable over Robinson.

Claim 4

Claim 4 recites in part "instructing the second party to decrypt the encrypted code of the transaction certificate based on a public key of the first party to generate decrypted selected

Appl. No. : 09/883,625
Filed : June 18, 2001

elements . . .” This feature is similar to those found in Claims 20 and 15 as discussed above. Accordingly, Claim 4 is additionally allowable for substantially similar reasons. In addition, Applicant submits that Robinson does not anticipate Claim 4 because it does not disclose at least “instructing the second party” as recited in the claim. The Office Action states that this feature is shown at “column 5, lines 41-53, customer obtains merchant public key can decrypt the transaction receipt.” Office Action at page 3.

At column 5, lines 41-53, Robinson states:

In the case where a public key cryptosystem is used in step 115, it is preferred that the merchant use its own secret key so that no other party may re-encrypt an altered version of the transaction record. If the merchant's own secret key is used to encrypt the transaction record in step 115, then the merchant need not keep the corresponding public key private. If a customer obtains the merchant's public key, for example, the customer could decrypt the transaction receipt, but would still be unable to re-encrypt an altered version of the receipt without the merchant's secret key. Alternatively, the merchant could use its public key for encryption in step 115, so long as the public key is not distributed.

Nowhere in this cited passage does Robinson indicate that the second party is instructed to decrypt the encrypted code of the transaction certificate as is recited in Claim 4. The passage poses a hypothetical situation in which a customer might obtain a public key and decrypt a transaction receipt, but the reference discloses no instruction to do so.

Given that there is no disclosure of instruction present in Robinson, it appears that the Examiner is relying inherency to find anticipation. However, as discussed above, “the missing descriptive matter [must be] necessarily present in the thing described in the reference.” *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999). Under MPEP 2112, an Examiner must provide rationale or evidence tending to show inherency. More particularly, the Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent feature necessarily flows from the teachings of the applied prior art. *Ex parte Levy*, 17 USPQ2d 1461, 1464 (BPAI 1990) (emphasis in original). To date, the Examiner has provided no such basis for finding the feature of instructing to be inherent in Robinson. Accordingly, the rejection of Claim 4 should be withdrawn.

Claim 22

-16-

Appl. No. : 09/883,625
Filed : June 18, 2001

Claim 22 also stands rejected as being anticipated by Robinson. Claim 22 recites in part "a first decryption module configured to decrypt the encrypted code to generate decrypted proof elements, based on a public key of the first party, wherein the decrypted proof elements are used to prove the transaction." As was discussed previously in connection with Claim 15, Robinson discloses that a customer hypothetically could obtain a merchant's public key and decrypt the transaction receipt. However, Robinson never discloses that any proof elements generated by the customer using the merchant's public key could be used for proving the transaction. The system contemplated by Robinson only contemplates a customer presenting a still encrypted receipt to a merchant. See Column 8, lines 38-57 ("In step 140, the customer presents a digital receipt page to the merchant computer In steps 144 and 146, the transaction record is decrypted by the merchant computer and the transaction information is extracted Since the transaction record was originally encrypted under the direction of the merchant, the merchant computer simply uses the same private key to extract the transaction data.") Thus, Robinson fails to teach or otherwise disclose the claimed feature of a first decryption module configured to "decrypt the encrypted code to generate decrypted proof elements, based upon a public key of the first party," where those decrypted proof elements are then used to prove the transaction as is recited in Claim 22. Thus, Claim 22 is also allowable over Robinson.

Discussion of Rejections Under 35 U.S.C. § 103(a)

Claims 1-3, 6-7, 11-14, and 17 and rejected under 35 U.S.C. § 103(a) as being unpatentable over Robinson in view of Zhao et al., U.S. Pat. No. 6,243,480 ("Zhao").

Claim 1

The Office Action states that Claim 1 is unpatentable over Robinson in view of Zhao. The Examiner concedes that Robinson does not disclose printing at least a portion of the received transaction elements on a hardcopy transaction certificate, nor does it disclose printing the encrypted code on the hardcopy transaction certificate and instructing the second party to scan the transaction certificate to convert the encrypted code to electronic form. The Office Action relies on Zhao stating that Zhao teaches receiving a hardcopy of a document with partial authentication information and scanning the analog reference to convert the encrypted code into an electronic form for verification, at column 3, line 57 – column 4, line 14. According to the

Appl. No. : 09/883,625
Filed : June 18, 2001

Office Action, it would have been obvious to one of ordinary skill in the art to print out a hardcopy of the transaction receipt to be scanned in at a later time to verify a transaction. As Zhao states, at column 3, lines 41-54, that such a modification would provide a way to authenticate a digital receipt that has been printed out without losing the authentication information.

Claim 1 recites in part "instructing the second party to scan the transaction certificate to convert the encrypted code to electronic form." Applicant submits that Claim 1 is allowable over the combination of Zhao and Robinson, even if proper, for at least the following reasons. First, neither Zhao nor Robinson teaches instructing the second party to do anything. Thus, the combination cannot read on Claim 1. Second, as discussed above in connection with Claims 4, 15 and 22, the passage relied upon by the Examiner to show decrypting encrypted code based on a public key of the first party is merely a hypothetical posed by Robinson and is expressly disclaimed, at column 6, lines 2-5. Moreover, as discussed above, decrypted selected elements in Robinson are used only by the first party (e.g., the merchant) to prove the transaction, not the second party as recited in Claim 1. Accordingly, Claim 1 is allowable.

Claim 14

Claim 14 also stands rejected over the combination of Zhao and Robinson. Applicant submits that, as with allowable Claims 4, 15 and 22, Claim 14 also includes the feature of "decrypting the converted encrypted code based on the retrieved public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." Applicant submits that the combination of Zhao and Robinson, even if proper, fails at least to teach decrypting the encrypted code based on the retrieved public key of the first party and using it to generate decrypted proof elements wherein those decrypted proof elements are used to prove the transaction. As discussed above in connection with Claim 15, Robinson fails to disclose using decrypted proof elements to prove the transaction because it shows only a system in which the merchant uses its private key to decrypt code and prove the transaction.

Appl. No. : 09/883,625
Filed : June 18, 2001

Claims 9, 10, 16, 21, and 23

Claims 9, 10, 16, 21, and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Robinson in view of Powar, U.S. Pat. No. 6,285,991 (Powar).

With respect to Claims 9 and 21, the Office Action concedes that Robinson does not disclose retrieving a public key of the second party to generate an encrypted transaction certificate; transmitting the encrypted transaction certificate to the second party; and instructing the second party to decrypt the transmitted encrypted transaction certificate based on a private key of the second party to produce a decrypted transaction certificate that includes the encrypted code. The Office Action instead relies on Powar, stating that Powar teaches sending a statement to a customer using a customer's public key system at column 4, line 55 to column 5, line 17, and at column 11, lines 1-50.

Applicant respectfully submits that the neither Robinson nor Powar, alone or in combination, teaches "instructing the second party to decrypt the transmitted encrypted transaction certificate" or "instructing the second party to decrypt the included encrypted code" as recited in Claim 9. Neither Robinson nor Powar teaches instructing a second party to do anything. Accordingly, Claim 9 is allowable over the combination of Robinson and Powar.

Regarding Claim 21, Applicant also submits that neither Robinson nor Powar, alone or in combination, disclose a system wherein an encrypted code is decrypted based on a public key of the first party to generate decrypted selected elements proof elements, and using proof elements generated in such a way for proving the transaction. The system contemplated by Robinson only contemplates a second party presenting a still encrypted receipt to a first party, wherein the first party then decrypts the receipt using its private key. See Column 8, lines 38-57 ("In step 140, the customer presents a digital receipt page to the merchant computer In steps 144 and 146, the transaction record is decrypted by the merchant computer and the transaction information is extracted Since the transaction record was originally encrypted under the direction of the merchant, the merchant computer simply uses the same private key to extract the transaction data.") Thus, Robinson and Powar fail to teach each element in Claim 21, and Claim 21 is allowable.

Claim 16 also stands rejected under the combination of Robinson and Powar. Claim 16 includes the recited feature of "decrypting the encrypted code based on the retrieved public key

BEST AVAILABLE COPY

Appl. No. : 09/883,625
Filed : June 18, 2001

of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action states that Robinson teaches this claimed feature. However, as was discussed above in connection with Claim 15, any use of decrypted proof elements to prove the transaction in Robinson occurs only after the vendor decrypts the proof elements using its own private key. Powar does not cure this deficiency. Accordingly, Claim 16 is allowable.

Claim 23 also stands rejected under Robinson and Powar. Claim 23 recites in part, "a second decryption module configured to decrypt the encrypted code based on a public key of the first party to generate decrypted proof elements, wherein the decrypted proof elements are used to prove the transaction." The Office Action states that Robinson teaches this feature at column 5, lines 41-53 and at columns 2, 6, and 7. Applicant submits that Robinson never discloses that any proof elements generated by a second decryption module based on a public key could be used for proving the transaction. The system contemplated by Robinson only contemplates a customer presenting a still encrypted receipt to a merchant. See Column 8, lines 38-57 ("In step 140, the customer presents a digital receipt page to the merchant computer In steps 144 and 146, the transaction record is decrypted by the merchant computer and the transaction information is extracted Since the transaction record was originally encrypted under the direction of the merchant, the merchant computer simply uses the same private key to extract the transaction data.") Thus, Robinson fails to teach or otherwise disclose the claimed feature of a second decryption module configured to "decrypt the encrypted code to generate decrypted proof elements, based upon a public key of the first party," where those decrypted proof elements are then used to prove the transaction as is recited in Claim 23. Powar does not cure this deficiency. Thus, Claim 23 is allowable.

Dependent Claims

Claims 2-3, 5-8 and 10-13 are dependent either directly or indirectly on one of the above-discussed independent claims. Applicant respectfully submits that pursuant to 35 U.S.C. § 112, ¶4, the dependent claims incorporate by reference all the limitations of the claim to which they refer and include their own patentable features, and are therefore in condition for allowance.

BEST AVAILABLE COPY

Appl. No. : 09/883,625
Filed : June 18, 2001

Therefore, Applicant respectfully requests the withdrawal of all claim rejections and prompt allowance of the claims.

Appl. No. : 09/883,625
Filed : June 18, 2001

BEST AVAILABLE COPY**CONCLUSION**

In light of the above, reconsideration and withdrawal of the outstanding rejections are specifically requested. In view of the foregoing remarks, Applicant respectfully submits that the claims of the above-identified application are in condition for allowance. However, if the Examiner finds any impediment to allowing all claims that can be resolved by telephone, the Examiner is respectfully requested to call the undersigned.

Please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: 5/15/06

By: 

John M. Carson
Registration No. 34,303
Attorney of Record
Customer No. 20,995
(619) 235-8550

AMEND

2599357
051506